UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/698,784	10/31/2003	John Apostolopoulos	200312858-1	1717

22879 7590 07/31/2008
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
ALMEIDA, DEVIN E	

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
07/31/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No. 10/698,784	Applicant(s) APOSTOLOPOULOS ET AL.	
	Examiner DEVIN ALMEIDA	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, 5-14, 18-30 and 32-34* is/are rejected.

7)□ Claim(s) *3,4,16,17 and 31* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 6/5/2007. Claims 1-34 were received for consideration.

Response to Arguments

Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 14, and 23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is unclear whether the data packets of the plurality of data packets have a first data segment or a plurality of first data segments. Also it is unclear whether the data packets of the plurality of data packets have one second data segment or a plurality of second data segments. For interpretation of art the claim are going to be read as each data packet having a first data segments and a second data segments. If the applicant wants each data packet comprising a plurality of first data segments and a plurality of second data segments. Examiner recommends amending the claims to read "*for a plurality of data packets <u>each</u> comprising a plurality of first data segments and a plurality of second data segments*".

Claim Rejections - 35 USC § 103

Claims 1, 2, 5-10, 12, 13, 23-30, and 32-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wee et al., "Secure Scalable Video Streaming for Wireless Networks," IEEE International Conference on Acoustics, Speech, and Signal Processing, Salt Lake City, Utah, May 2001, (hereinafter Wee) in view of Kang, U.S. 5,958,080 (hereinafter Kang) in further view of Miller et al., U.S. Patent No. 5,790,669 (hereinafter Miller).

Regarding claim 1: Wee discloses a method (page 1 col. 2 ¶2) for ensuring the integrity of data, comprising:

for a plurality of data packets comprising a plurality of first data segments and a plurality of second data segments (page 3 col. 1 ¶2),

wherein said plurality of first data segments have a different priority than said plurality of second data segment (page 3 col.2 ¶2 i.e. Progressive encryption methods have the property that smaller blocks of data are encrypted progressively. While block code encryption with small block sizes is not very secure, progressive encryption methods add a degree of security by feeding encrypted data of earlier blocks into the encryption of a later block~ Decryption can then be performed progressively as well. The first small block of cipher text can be decrypted into plaintext by itself while later blocks of cipher text depend on the decrypted plaintext from earlier blocks. Thus, earlier blocks of cipher text can be decrypted without knowledge of the entire cipher next segment. This progressive nature of cipher block chains and stream ciphers matches nicely with the progressive or embedded nature of scalable coding. It is this combination that enables efficient secure transcending operations to be performed in SSS.).

Wee does not disclose calculating cryptographic checksums for said plurality of said first data segments, such that a data packet of said plurality of data packets is associated with a plurality of said cryptographic checksums; and enabling said cryptographic checksum for said plurality of said first data segments to be transmitted separately from said plurality of data packets (see column 6 lines 15-41).

Kang discloses calculating a cryptographic checksum for said plurality of said first data segments, such that a data packet of said plurality of data packets is associated with a plurality of said cryptographic checksums. Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the plurality of checksums for each packet as a way to make that not only the checksum of the packet match but also the checksum of the plurality of packet match (see column 6 lines 15-41).

Miller discloses calculating a cryptographic checksum for said plurality of said first data segments (col. 1 lines 27-44); and enabling said cryptographic checksum for said plurality of said first data segments to be transmitted separately from said plurality of data packets (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

Regarding claim 2: Wee discloses a plurality of said second data segments (page 3 col. 1 ¶2).

Wee does not disclose calculating a cryptographic checksum; and enabling said cryptographic checksum for said plurality of said second data segments to be transmitted separately from said plurality of data packets.

Miller discloses calculating a cryptographic checksum (col. 1 lines 27-44); and enabling said cryptographic checksum for said plurality of said second data segments to be transmitted separately from said plurality of data packets (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

Regarding claim 5: Wee discloses an opportunistic integrity checking scheme (page 1 col. 1 ¶3).

Regarding claim 6: Wee does not disclose that said calculating of said cryptographic checksum is performed using a technique selected from the group consisting of: a hash function providing a fingerprint of data contained in an encrypted data packet and which guarantees the authenticity of received data and the validity of decrypted data, Message Authentication Codes (MAC), Message Digest algorithms, keyed hashes, SHA (Secure Hash Algorithm), RIPEMD (RACE Integrity Primitives Evaluation Message Digest), HMAC (keyed-Hashing for Message Authentication), and digital signature schemes.

Miller discloses that said calculating of said cryptographic checksum is performed using the techniques of: a hash function providing a fingerprint of data contained in an encrypted data packet and which guarantees the authenticity of received data and the validity of decrypted data (col. 7 lines 40-44), and digital signature schemes (col. 1-2 lines 60-4).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

Regarding claims 7 and 18: Wee discloses that said plurality of said data packets comprises secure scalably streamable data (Title).

Regarding claim 8: Wee discloses that said plurality of said data packets include data comprising scalably compressed data for media selected from the group consisting of: speech, audio, image (*see* 5.1: Scalable Coding – Packetization), video (page 1 col. 1 ¶2), and computer graphics.

Regarding claim 9: Wee discloses that said plurality of said data packets include data scalably formatted according to the techniques of: JPEG-2000 (page 2 col. 1 ¶5) with spatial scalability (page 3 col. 1 ¶1 and ¶3); MPEG-1/2/4 (page 2 col. 1 ¶5) or H.261/2/3/4 (page 2 col. 1 ¶5) using spatial scalability (page 3 col. 1 ¶1 and ¶3); and progressive/scalable graphics compression (page 3 §5.1).

Regarding claims 10 and 19: Wee discloses that said plurality of said data packets comprises media data (page 3 col. 1 ¶2).

Regarding claims 12 and 21: Wee discloses encrypting one or more data packets (pages 3-4 §5.2).

Regarding claims 13 and 22: Wee and Miller disclose said cryptographic checksum as indicated regarding claim 1, above. Wee further discloses encrypting (pages 3-4 §5.2).

Regarding claim 23: Wee discloses an apparatus for ensuring integrity of data, comprising:

a receiver for receiving a first plurality of data packets and a second plurality of data packets, each of said packets comprising a plurality of data segments (page 1 col. 1 ¶2) wherein data segments of said plurality of first data packets have a different priority than data segments of said plurality of second data packets (page 3 col.2 ¶2 i.e. Progressive encryption methods have the property that smaller blocks of data are encrypted progressively. While block code encryption with small block sizes is not very secure, progressive encryption methods add a degree of security by feeding encrypted data of earlier blocks into the encryption of a later block~ Decryption can then be performed progressively as well. The first small block of cipher text can be decrypted into plaintext by itself while later blocks of cipher text depend on the decrypted plaintext from earlier blocks. Thus, earlier blocks of cipher text can be decrypted without knowledge of the entire cipher next segment. This progressive nature of cipher block chains and stream ciphers matches nicely with the progressive or embedded nature of scalable coding. It is this combination that enables efficient secure transcending operations to be performed in SSS.).

Wee does not disclose a cryptographic checksum calculator coupled to said receiver, said cryptographic checksum calculator for calculating a cryptographic checksum for each of said data segments; or a cryptographic checksum appender coupled to said cryptographic checksum calculator for assembling said cryptographic checksum.

Miller discloses a cryptographic checksum calculator coupled to said receiver, said cryptographic checksum calculator for calculating a cryptographic checksum for one or more of said data segments (col. 1 lines 27-44); and a cryptographic checksum appender coupled to said cryptographic checksum calculator for assembling said cryptographic checksum (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

Regarding claim 24: Wee discloses a plurality of data packets comprising a plurality of first data segments and a plurality of second data segments (page 3 col. 1 ¶2).

Wee does not disclose that said cryptographic checksum calculator is enabled to calculate a cryptographic checksum for said plurality of said first data segments; or to enable said cryptographic checksum for said plurality of said first data segments to be transmitted separately from said plurality of data packets.

Miller discloses that said cryptographic checksum calculator is enabled to calculate a cryptographic checksum for said plurality of said first data segments (col. 1 lines 27-44); and to enable said cryptographic checksum for said plurality of said first data segments to be transmitted separately from said plurality of data packets (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

Regarding claim 25: Wee does not disclose that said cryptographic checksum calculator is enabled to calculate said cryptographic checksum for said set of said data segments independently of cryptographic checksums calculated for other sets of said data segments.

Miller discloses that said cryptographic checksum calculator is enabled to calculate said cryptographic checksum for said set of said data segments independently of cryptographic checksums calculated for other sets of said data segments (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

Regarding claim 26: Wee discloses a forwarder for forwarding said packets to a destination (page 1-2 §2).

Regarding claim 27: Wee discloses a method for ensuring integrity of data, comprising:

receiving a data packet comprising an amount of data partitioned into a plurality of data segments (page 1 col. 1 ¶2), wherein said plurality of first data segments have a different priority than said plurality of second data segment (page 3 col.2 ¶2 i.e. Progressive encryption methods have the property that smaller blocks of data are encrypted progressively. While block code encryption with small block sizes is not very secure, progressive encryption methods add a degree of security by feeding encrypted data of earlier blocks into the encryption of a later block~ Decryption can then be performed progressively as well. The first small block of cipher text can be decrypted into plaintext by itself while later blocks of cipher text depend on the decrypted plaintext from earlier blocks. Thus, earlier blocks of cipher text can be decrypted without knowledge of the entire cipher next segment. This progressive nature of cipher block chains and stream ciphers matches nicely with the progressive or embedded nature of scalable coding. It is this combination that enables efficient secure transcending operations to be performed in SSS.).

Wee does not disclose calculating a cryptographic checksum for a first of said plurality of data segments; or enabling said cryptographic checksum for said first of said plurality of data segments to be transmitted separately from said data packet.

Miller discloses calculating a cryptographic checksum for a first of said plurality of data segments (col. 1 lines 27-44); and enabling said cryptographic checksum for said first of said plurality of data segments to be transmitted separately from said data packet (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

Regarding claim 28: Wee discloses said first data segment and a second of said plurality of data segments (page 3 col. 1 ¶2). Wee does not disclose calculating cryptographic checksums. Miller discloses calculating cryptographic checksums (col. 1 lines 27-44).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

Regarding claim 29: Wee discloses a method for ensuring integrity of data, comprising: receiving a data packet comprising an amount of data partitioned into at least a first data segment (page 1 col. 1 ¶2) wherein said plurality of first data segments have a different priority than said plurality of second data segment (page 3 col.2 ¶2 i.e. Progressive encryption methods have the property that smaller blocks of data are encrypted progressively. While block code encryption with small block sizes is not very secure, progressive encryption methods add a degree of security by feeding encrypted data of earlier blocks into the encryption of a later block~ Decryption can then be performed progressively as well. The first small block of cipher text can be decrypted into plaintext by itself while later blocks of cipher text depend on the decrypted plaintext from earlier blocks. Thus, earlier blocks of cipher text can be decrypted without knowledge of the entire cipher next segment. This progressive nature of cipher block chains and stream ciphers matches nicely with the progressive or embedded nature of scalable coding. It is this combination that enables efficient secure transcending operations to be performed in SSS.).

Wee does not disclose calculating a cryptographic checksum for said at least one data segment; or enabling said cryptographic checksum for said at least one data segment to be transmitted separately from said data packet.

Miller discloses calculating a cryptographic checksum for said at least one data segment (col. 1 lines 27-44); and enabling said cryptographic checksum for said at least one data segment to be transmitted separately from said data packet. (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

Regarding claim 30: Wee does not disclose calculating a second cryptographic checksum for a second of said at least one data segment; and enabling said cryptographic checksum for said at least one data segment to be transmitted separately from said data packet.

Miller discloses calculating a second cryptographic checksum for a second of said at least one data segment (col. 1 lines 27-44); and enabling said cryptographic checksum for said at least one data segment to be transmitted separately from said data packet (col. 2-3 lines 58-16).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

Regarding claim 32: Wee discloses an apparatus for verifying the integrity of data, comprising: a receiver, said receiver configured to receive first data second data and a previously determined cryptographic checksum corresponding to said data (page 1 col. 1 ¶2) wherein said plurality of first data segments have a different priority than said plurality of second data segment (page 3 col.2 ¶2 i.e. Progressive encryption methods have the property that smaller blocks of data are encrypted progressively. While block code encryption with small block sizes is not very secure, progressive encryption methods add a degree of security by feeding encrypted data of earlier blocks into the encryption of a later block~ Decryption can then be performed progressively as well. The first small block of cipher text can be decrypted into plaintext by itself while later blocks of cipher text depend on the decrypted plaintext from earlier blocks. Thus, earlier blocks of cipher text can be decrypted without knowledge of the entire cipher next segment. This progressive nature of cipher block chains and stream ciphers matches nicely with the progressive or embedded nature of scalable coding. It is this combination that enables efficient secure transcending operations to be performed in SSS.).

Wee does not disclose an integrity check module coupled to said receiver, said integrity check module configured to calculate a new cryptographic checksum corresponding to said received data and to determine whether said new cryptographic checksum matches said previously determined cryptographic checksum.

Miller discloses an integrity check module coupled to said receiver, said integrity check module configured to calculate a new cryptographic checksum corresponding to said received data and to determine whether said new cryptographic checksum matches said previously determined cryptographic checksum (col. 1 lines 27-44).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

Regarding claim 33: Wee does not disclose that said integrity check module is integral with said receiver. Miller discloses that said integrity check module is integral with said receiver (col. 1 lines 27-44).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

Regarding claim 34: Wee does not disclose an output coupled to said integrity check module, said output configured to provide an indication of whether said new cryptographic checksum matches said previously determined cryptographic checksum.

Miller discloses an output coupled to said integrity check module, said output configured to provide an indication of whether said new cryptographic checksum matches said previously determined cryptographic checksum (col. 1 lines 27-44).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify Wee by the computationally lightweight method & system as taught by Miller in order to create a more efficient data verification system (*see* Miller col. 2 lines 5-14).

Claims 11, 14-15, 18-22, are rejected under 35 U.S.C. 103(a) as being unpatentable over Wee in view of Kang in view of Miller and further in view of Doyle et al., U.S. Patent Publication No. 2002/0095586 A1 (hereinafter Doyle).

Regarding claim 14: The combination of Wee and Miller discloses a method for ensuring the integrity of data, comprising: for a plurality of data packets comprising a plurality of first data segments and a plurality of second data segments, calculating a cryptographic checksum for said plurality of said first data segments, such that a data packet of said plurality of data packets is associated with a plurality of said cryptographic checksums, wherein said plurality of first data segments have a different priority than said plurality of second data segment; and enabling said cryptographic checksum for said plurality of said first data segments to be transmitted separately from said plurality of said data packets, as indicated regarding claim 1, above.

Neither Wee, Kang nor Miller discloses a computer readable medium having instructions stored therein for implementing said method. Doyle discloses a computer readable medium having instructions stored therein for implementing said method (Abstract).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to implement the combination Wee and Miller via the technique taught by Doyle in order to conveniently and economically distribute operational copies of the software embodying the method to multiple computing devices (*see* Doyle [0018]).

Regarding claims 11 and 20: The combination of Wee and Miller, as indicated regarding claims 1 and 14, above, does not disclose that said data is stored in a storage medium. Doyle discloses that said data is stored in a storage medium [0003] and [0005].

Therefore, it would have been obvious to one skilled in the art at the time of the invention to implement the combination Wee and Miller via the technique taught by Doyle in order to create a more computationally efficient data verification system (*see* Doyle [0018] and Miller col. 2 lines 5-14).

Claim 15 is rejected as per reasons regarding claim 2 further in view of Doyle, above.

Claim 18 is rejected as per reasons regarding claim 7 further in view of Doyle, above.

Allowable Subject Matter

Claims 3, 4, 16, 17 and 31 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Devin Almeida/
Examiner, Art Unit 2132
8/8/2007

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132